Amenazas y vulnerabilidades de la seguridad informática

Clasificación general de amenazas

En el campo de la seguridad informática se maneja mucho el término de "amenaza". El diccionario de la lengua española la define como el "anuncio de un mal o peligro" En términos generales, existen dos tipos de amenazas, las que provienen de sucesos naturales, como por ejemplo; terremotos, incendios forestales, huracanes, inundaciones, sequías, plagas, tsunamis y tornados y las amenazas provocadas por la actividad humana, como las explosiones, los incendios, los derrames de sustancias tóxicas, las guerras, el terrorismo, entre otros.

Dentro de las amenazas provocadas por la actividad humana relacionada con la seguridad informática, se puede decir que, una amenaza representa la acción que tiende a causar un daño a los dispositivos o sistemas en donde se encuentra almacenada la información, atentando contra su confidencialidad, integridad y disponibilidad.
Si una amenaza se llega a efectuar, ocurren diversos casos como por ejemplo; interrupción de un servicio o procesamiento de un sistema, modificación o eliminación de la información, daños físicos, robo del equipo y medios de almacenamiento de la información, entre otros. Las amenazas a la seguridad informática se clasifican en humanas, lógicas y físicas.

- **Humanas**

Estos ataques provienen de individuos que de manera intencionada o no, causan enormes pérdidas aprovechando alguna de las vulnerabilidades que los sistemas puedan presentar. A estas personas se les bautizó de la siguiente manera, derivado del perfil que presenta cada individuo y para el presente trabajo únicamente se dan a conocer las más importantes las cuales se describen a continuación:

- ✓ **Hacker:** Persona que vive para aprender y todo para él es un reto, es curioso y paciente, no se mete en el sistema para borrarlo o para vender lo que consiga, quiere aprender y satisfacer su curiosidad. Crea más no destruye.

- ✓ **Cracker:** Es un hacker cuyas intenciones van más allá de la investigación, es una persona que tiene fines maliciosos, demuestran sus habilidades de forma equivocada ó simplemente hacen daño sólo por diversión.
- ✓ **Phreakers:** Personas con un amplio conocimiento en telefonía, aprovechan los errores de seguridad de las compañías telefónicas para realizar llamadas gratuitas.

No se necesita ser un hacker para realizar alguna acción maliciosa a los sistemas de información, muchas veces un individuo puede realizar una acción indebida por diversión, por desconocimiento, entre otros. Hay que recordar que el talón de Aquiles de una empresa es su propio personal, es por ello que han surgido nuevos sistemas de ataque, los cuales se describen a continuación:

- ✓ **Ingeniería social:** Un atacante utiliza la interacción humana o habilidad social para obtener información comprometedora acerca de una organización, de una persona o de un sistema de cómputo. El atacante hace todo lo posible para hacerse pasar por una persona modesta y respetable, por ejemplo, pretende ser un nuevo empleado, un técnico de reparación, un investigador, etc.
- ✓ **Ingeniería social inversa:** El atacante demuestra de alguna manera que es capaz de brindar ayuda a los usuarios y estos lo llaman ante algún imprevisto, aprovechando la oportunidad para pedir la información necesaria y así solucionar el problema tanto del usuario como el propio.
- ✓ **Trashing (cartoneo):** Generalmente, un usuario anota su login y pasword en un papelito y luego, cuando lo recuerda, lo arroja a la basura. El trashing puede ser físico (como el que se describió) o lógico, como analizar buffers de impresora y memoria bloques de discos, entre otros.
- ✓ **Terroristas:** No se debe de entender a los que se dedican a poner bombas o quemar autobuses; bajo esta definición se engloba a cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en él.
- ✓ **Robo:** La información contenida en los equipos de cómputo puede copiarse fácilmente, al igual que los discos magnéticos y el software.
- ✓ **Intrusos remunerados:** Es el grupo de atacantes de un sistema más peligroso aunque es el menos habitual en las redes normales ya que suele afectar más a las grandes empresas u organismos de defensa. Se trata de personas con gran experiencia en problemas de seguridad y con un amplio conocimiento del sistema, que son pagados por una tercera parte generalmente para robar secretos o simplemente dañar la imagen de la entidad afectada.

- ✓ **Personal interno:** Son las amenazas al sistema, provenientes del personal del propio sistema informático, rara vez es tomado en cuenta porque se supone un ámbito de confianza muchas veces inexistente. Este tipo de ataque puede ser causado de manera intencional o sin dolo.
- ✓ **Ex–Empleados:** Se trata de personas descontentas con la organización que aprovechan las debilidades de un sistema que conocen perfectamente, para dañarlo como venganza por algún hecho que consideran injusto.
- ✓ **Curiosos:** Personas con un alto interés en las nuevas tecnologías, pero no cuentan con la suficiente experiencia para ser considerados como hackers o crackers.
- ✓ **Personal interno:** Las amenazas a la seguridad de un sistema, provenientes del personal del propio sistema informático, rara vez es tomada en cuenta, porque se supone un ámbito de confianza muchas veces inexistente. Estos ataques son accidentes por desconocimiento o inexistencia de las normas básicas de seguridad; pero también son de tipo intencional. Por ejemplo: un electricista puede ser más dañino que el más peligroso de los delincuentes informáticos, ya que un corte de energía puede causar un desastre en los datos del sistema.

- **Lógicas**

En este tipo de amenazas se encuentran una gran variedad de programas que, de una u otra forma, dañan los sistemas creados de manera intencionada (software malicioso conocido como malware) o simplemente por error (bugs o agujeros).

Las amenazas más comunes son:

- ✓ **Adware:** Software que durante su funcionamiento despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes o a través de una barra que aparece en la pantalla.
- ✓ **Backdoors:** Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar 'atajos' en los sistemas de autenticación del programa o del núcleo que se está diseñando. A estos atajos se les denomina puertas traseras y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos.
- ✓ **Bombas Lógicas:** Son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.

- ✓ **Caballos de Troya:** Es aquel programa que se hace pasar por un programa válido cuando en realidad es un programa malicioso. Se llama troyano, caballo de Troya (trojan horse) por la semejanza con el caballo que los griegos utilizaron para disfrazar su identidad y ganar su guerra contra la ciudad de Troya. Así, un usuario podría descargar de un sitio Web de Internet un archivo de música que en realidad es un troyano que instala en su equipo un keylogger o programa que capture todo lo que escriba el usuario desde el teclado y después esta información sea enviada a un atacante remoto.
- ✓ **Exploits:** Programa o técnica (del ingles to exploit, explotar, aprovechar) que aprovecha una vulnerabilidad. Los exploits dependen de los sistemas operativos y sus configuraciones.
- ✓ **Gusanos (Worms):** Programas que se propagan por sí mismos a través de las redes, tomando ventaja de alguna falla o hueco de seguridad en los sistemas operativos o en el software instalado en los equipos de cómputo y que tiene como propósito realizar acciones maliciosas.
- ✓ **Malware:** Proviene de la agrupación de las palabras **"Mal**icious Soft**ware".** Este programa o archivo, está diseñado para insertar virus, gusanos, troyanos, spyware o incluso bots (tipo de troyano que cumple una función específica), intentando conseguir información sobre el usuario o sobre la PC.
- ✓ **Pharming:** Consiste en suplantar el Sistema de Resolución de Nombres de Dominio (DNS, Domain Name System) con el propósito de conducir al usuario a una página Web falsa.
- ✓ **Phishing:** Es un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria. El estafador, mejor conocido como phisher se hace parar por una persona o empresa de confianza en una aparente comunicación oficial electrónica.
- ✓ **Spam:** Mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas. La más utilizada entre el público en general es la basada en el correo electrónico. El spam también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea.
- ✓ **Spyware o programas espía:** Se refiere a las aplicaciones que recopilan información sobre una persona u organización, las cuales se instalan y se ejecutan sin el conocimiento del usuario. El objetivo principal del spyware es recolectar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas.

- ✓ **Virus:** Programas que tienen como objetivo alterar el funcionamiento de la computadora y en ciertos casos alterar la información, se propagan sin el consentimiento y conocimiento del usuario. Algunos de los virus informáticos requieren de la intervención del usuario para comenzar a propagarse, es decir, no se activan por sí mismos, otros no la requieren y se activan solos.

En un principio, los virus se propagaban a través del intercambio de dispositivos de almacenamiento como disquetes y memorias de almacenamiento (USBs). Actualmente un equipo se puede infectar al abrir un archivo adjunto (ya sean documentos, imágenes, juegos, entre otros.) que llegue a través de un correo electrónico.

Los virus se distribuyen a través de mecanismos de intercambio de archivos, es decir, aquellos que se suelen utilizar para distribuir software, música y videos, están diseñados para afectar a los sistemas operativos. La manera de erradicarlos y de protegerse contra éstos, es a través de un software antivirus, éste vendría siendo de poca ayuda si no se encuentra actualizado.

Dentro de este tipo de ataque (lógico), existen otro tipo de ataques los cuales tienen que ver con los sistemas y se han clasificado de la siguiente manera:

- ✓ **Ataques de Autenticación:** Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y Pasword. Algunos de estos ataques son: **Spoofing-Looping** (los ataques tipo Spoofing bastante conocidos son el IP Spoofing, el DNS Spoofing y el Web Spoofing), **IP Splicing-Hijacking, Spoofing (**Existen los IP Spoofing, DNS spoofing y Web Spoofing), **Net Flooding.**
- ✓ **Ataques de Monitorización:** Se realiza para observar a la víctima y su sistema, con el objetivo de establecer sus vulnerabilidades y posibles formas de acceso futuro. Se presentan como: **Shoulder Surfing, Decoy (Señuelos), Scanning (búsqueda), Snooping-Downloading, TCP Connect Scanning, TCP SYN Scanning.**
- ✓ **Uso de Diccionarios:** Son archivos con millones de palabras, las cuales pueden ser passwords utilizadas por los usuarios. El programa encargado de probar cada una de las palabras encripta cada una de ellas (mediante el algoritmos utilizado por el sistema atacado) y compara la palabra encriptada contra el archivo de passwords del sistema atacado (previamente obtenido). Si coinciden se ha

encontrado la clave de acceso al sistema mediante el usuario correspondiente a la clave hallada.

- ✓ **Denial of Service (DoS):** Los ataques de denegación de servicio tienen como objetivo saturar los recursos de la víctima, de forma tal que se inhabilitan los servicios brindados por la misma. Ejemplos: **Jamming o Flooding, Syn Flood, Connection Flood, Net Flood, Land Attack, Smurf o Broadcast storm, Supernuke o Winnuke, Teardrop I y II, Newtear-Bonk-Boink, E-mail bombing-Spamming.**
- ✓ **Ataques de Modificación-Daño:** Se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima (incluyendo borrado de archivos). Ejemplos de este tipo de Ataques: **Tampering o Data Diddling, Borrado de Huellas. Ataques mediante Java Applets, Ataques Mediante JavaScript y VBScript, Ataques Mediante Active X, Ataques por Vulnerabilidades en los Navegadores.**

- **Físicos**

Este tipo de ataque está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en el cual se encuentran ubicados los centros de cómputo de cada organización o individuo. Las principales amenazas que se prevén en la seguridad física son:

- ✓ **Incendios:** Generalmente son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas. El fuego es una de las principales amenazas contra la seguridad porque es considerado como el enemigo número uno de las computadoras debido a que puede destruir fácilmente los archivos de información y programas. Por ello es necesario proteger los equipos de cómputo, instalándolos en áreas que cuenten con los mecanismos de ventilación y detección adecuados contra incendios y que únicamente ingrese el personal autorizado.
- ✓ **Inundaciones:** Se define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial.
- ✓ **Terremotos:** Fenómenos sísmicos que pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas.
- ✓ **Señales de Radar:** Las señales muy fuertes de radar infieren en el procesamiento electrónico de la información, pero únicamente si la señal que alcanza el equipo es de 5 volts/Metro o mayor. Ello podría ocurrir sólo si la antena respectiva fuera visible dese una ventana del

centro de procesamiento respectivo y en algún momento estuviera apuntando directamente hacia dicha ventana.

- ✓ **Instalaciones eléctricas:** Trabajar con computadoras implica trabajar con electricidad. En las instalaciones eléctricas se debe considerar los siguientes aspectos: picos y ruidos electromagnéticos, buen cableado, pisos de placas extraíbles, un buen sistema de aire acondicionado, emisiones electromagnéticas.

Esta clasificación, de los principales ataques a la seguridad informática van muy ligadas, son aspectos que no deben pasar desapercibidas en ninguna organización ya que conforman la base para tener una buena estructura de seguridad, si alguna de éstas falla, no se podrá tener la certeza de mantener protegida la información, lo que puede provocar grandes daños tanto económicos.

Clasificación general de vulnerabilidades

En materia de seguridad informática los puntos débiles de los sistemas son comúnmente aprovechados por personas que buscan la manera de acceder y realizar alguna acción maliciosa para su propio beneficio, desgraciadamente todos los sistemas tecnológicos presentan alguna debilidad, por ejemplo, los sistemas requieren de energía eléctrica, sin ella simplemente no funcionan.

Es por ello que es muy importante conocer esos puntos débiles, una vez identificados, las empresas definen las medidas de seguridad adecuadas con la finalidad de reducir los riesgos a los que pueda estar sometida, evitando que se efectúe una amenaza.

Estos puntos débiles se conocen como vulnerabilidades, el diccionario de la real academia de la lengua española define la palabra vulnerable como: "Que puede ser herido o recibir lesión física o moralmente". En materia de seguridad informática las vulnerabilidades son las debilidades de los activos de las organizaciones, las cuales podrían ser utilizadas por las amenazas para causar daño a los sistemas.

En la figura 2.1 se muestra una clasificación de las principales vulnerabilidades a las que las organizaciones están expuestas:

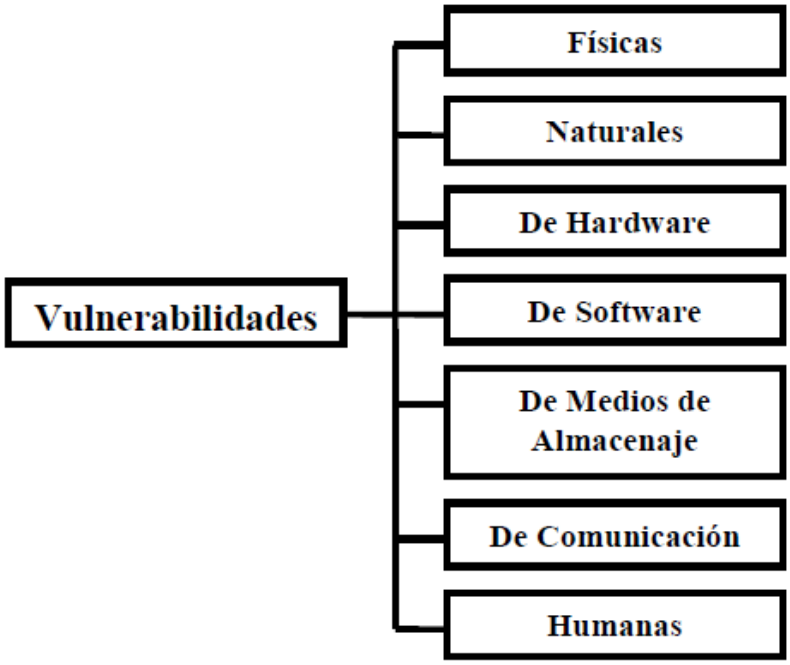

Figura 2.1 Principales Vulnerabilidades

A continuación se describirán de manera general cada uno de los diferentes tipos de vulnerabilidades:

- ✓ **Vulnerabilidad física**: Se refiere al lugar en donde se encuentra almacenada la información, cómo los centros de cómputo. Para un atacante le pue de resultar más sencillo acceder a la información que se encuentra en los equipos que intentar acceder vía lógica a éstos o también se puede dar el caso de que al acceder a los centros de cómputo el atacante quite el suministro de energía eléctrica, desconecte cables y robe equipos. Si este tipo de vulnerabilidad se llega a efectuar, afecta a uno de los principios básicos de la seguridad informática que es la disponibilidad.
- ✓ **Vulnerabilidad natural:** Se refiere a todo lo relacionado con las condiciones de la naturaleza que ponen en riesgo la información. Por ejemplo, incendios, inundaciones, terremotos, huracanes, entre otros. Por ello es conveniente contar con las medidas adecuadas, como tener respaldos, fuentes de energía alterna y buenos sistemas de ventilación, para garantizar el buen funcionamiento de los equipos.
- ✓ **Vulnerabilidad de hardware:** Hacen referencia a los posibles defectos de fábrica o a la mala configuración de los equipos de cómputo de la empresa que puedan permitir un ataque o alteración de éstos. Por ejemplo; la falta de actualización de los equipos que se

utilizan o la mala conservación de los equipos son factores de riesgo para las empresas.

- ✓ **Vulnerabilidad de software:** Está relacionado con los accesos indebidos a los sistemas informáticos sin el conocimiento del usuario o del administrador de red. Por ejemplo; la mala configuración e instalación de los programas de computadora, pueden llevar a un uso abusivo de los recursos por parte de usuarios mal intencionados. Los sistemas operativos son vulnerables ya que ofrecen una interfaz para su configuración y organización en un ambiente tecnológico y se realizan alteraciones en la estructura de una computadora o de una red.
- ✓ **Vulnerabilidad de medios de almacenaje:** Son los soportes físicos o magnéticos que se utilizan para almacenar la información. Por ejemplo; los disquetes, cd-roms, cintas magnéticas, discos duros, entre otros. Por lo tanto si estos soportes no se utilizan de manera adecuada, el contenido de los mismos podrá ser vulnerable a una serie de factores que afectan la integridad, disponibilidad y confidencialidad de la información.
- ✓ **Vulnerabilidad de comunicación:** Es el trayecto de la información, es decir, donde sea que la información viaje, ya sea vía cable, satélite, fibra óptica u ondas de radio, debe existir seguridad. El éxito en el tránsito de los datos es un aspecto crucial en la implementación de la seguridad de la información por lo tanto se debe evitar:

- Cualquier falla en la comunicación que provoque que la información no esté disponible para los usuarios, o por el contrario, que esté disponible para quien no tiene autorización.
- Que la información sea alterada afectando la integridad de ésta.
- Que la información sea capturada por usuarios no autorizados, afectando su confidencialidad.

- ✓ **Vulnerabilidad humana:** Se refiere a los daños que las personas puedan causar a la información y al ambiente tecnológico que la soporta sea de manera intencional o no. Muchas veces los errores y accidentes que amenazan a la seguridad de la información ocurren en ambientes institucionales, la principal vulnerabilidad es la falta de capacitación y la falta de conciencia de seguridad para las actividades de rutina, los errores, omisiones, etc. También existen las vulnerabilidades humanas de origen externo, como son; el vandalismo, estafas, invasiones, etc.

Las vulnerabilidades están ligadas a los hombres, a los equipos y al entorno. Por ejemplo, en cualquier organización de nada serviría tener herramientas de seguridad como (firewall's, IDS, antivirus, entre otros) si los centros de cómputo estuviesen en un lugar inadecuado y accesible a cualquier

gente, ya que se está expuesto a que cualquier individuo realice un uso indebido a los equipos provocando grandes daños.

Existen otros tipos de vulnerabilidades que también afectan a las organizaciones a nivel mundial, pero que muy difícilmente se toman en cuenta, estas son:

- ✓ **Vulnerabilidad de tipo Económico:** Se refiere a la escasez y un mal manejo de los recursos destinados a las organizaciones para el mejoramiento de las diversas áreas.
- ✓ **Vulnerabilidad de tipo Socio-Educativa:** Se refiere a las relaciones, comportamientos, métodos y conductas de todas aquellas personas que tienen acceso a una red y lo que deseen de ésta.
- ✓ **Vulnerabilidad de tipo Institucional/Política:** Se refiere a los procesos, organizaciones, burocracia, corrupción y autonomía que tienen todos los países del mundo. Desgraciadamente un atacante puede someter a ciertas personas a revelar información, realizando actos de corrupción.

Por lo anterior mencionado se puede decir que una vulnerabilidad es el paso previo a que se efectúe una amenaza, ésta se encuentra presente en todo momento, pero se reducen los riesgos teniendo en cuenta buenas medidas de seguridad.

Es recomendable que las empresas realicen análisis de riesgos detallado de las vulnerabilidades a las que están expuestos, como las físicas, de software, humanas, entre otros, para evitar en la medida de lo posible ser puntos blancos de ataque.

Es muy importante ser consciente de que por más que las empresas sean las más seguras desde el punto de vista de ataques externos, Hackers, virus, entre otros, la seguridad de la misma sería nula si no se ha previsto como combatir un incendio.

Por ello se hace mucho hincapié sobre la importancia de la seguridad informática, ya que se está invirtiendo para proteger el objeto más valioso de cualquier empresa, que es la información.

REFERENCIAS

Capítulo 2. "Amenazas y vulnerabilidades de la seguridad informática, recuperado" de: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/217/A5.pdf?sequence=5